THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION

PATRICK RUFFINO, on behalf of himself and all others similarly situated, Plaintiff, v. CAPITAL ONE FINANCIAL CORPORATION, CAPITAL ONE, N.A., AND CAPITAL ONE BANK (USA) Defendants.	Case No.: **JURY TRIAL DEMANDED**

CLASS ACTION COMPLAINT

Plaintiff Patrick Ruffino, on behalf of himself and all persons similarly situated, by and through his attorneys, alleges personal knowledge as to all facts related to himself and on information and belief as to all other matters, which are based upon, among other things, the investigation made by Plaintiff through his counsel:

PRELIMINARY STATEMENT

1. Plaintiff Patrick Ruffino ("Plaintiff") brings this action on behalf of himself and all other similarly situated Capital One credit card holders whose personal information hackers misappropriated and disseminated as a direct and proximate result of Defendants' Capital One Financial Corporation, Capital One Bank (USA), and Capital One, National Association (collectively, "Capital One" or "Defendants") failure to use reasonable care to secure and safeguard consumers' personal information. The compromised data includes full names, social security numbers, addresses, phone numbers, email addresses, dates of birth, credit scores, credit

limits, account balances, payment histories, social security numbers, and bank account numbers (the “Personal Data”).

2. On July 29, 2019 Capital One announced that it had suffered a catastrophic data breach of its information technology ("IT") system (the "Breach") carried out by Paige A. Thomas between March 23 and 24, 2019.[1]

3. News reports indicate consumers who held “secured” Capital One credit cards like that issued to and maintained by Plaintiff are most at risk. Because Capital One required Plaintiff and other secure card holders to provide their personal bank account information in order to receive a card, hackers and others may now have access to not only their personally identifiable information, but also sensitive bank account information. Capital One’s myriad failures have exposed secure card holders like Plaintiff to an exponentially greater risk of identify theft and fraud.

4. Capital One experienced this catastrophic data breach because it failed to develop, maintain, and implement sufficient security measures on the relevant databases, its representations to the contrary notwithstanding. Indeed, this Breach follows in the wake of a number of widely publicized data breaches affecting companies such as Anthem, Target, Home Depot, Neiman Marcus, Community Health Systems, Inc., Michaels Stores, Jimmy Johns, Sony Entertainment, J.P. Morgan Chase & Co., P.F. Chang’s, Staples, and others. But notwithstanding these earlier data security incidents, Defendants failed to take adequate steps to prevent the Breach from occurring.

5. Accordingly, Plaintiff brings this action for monetary, injunctive and declaratory relief.

[1] https://www.wired.com/story/capital-one-hack-credit-card-application-data/ (last visited July 31, 2019).

JURISDICTION AND VENUE

6. This Court has jurisdiction of this action pursuant to 28 U.S.C. § 1332 of the Class Action Fairness Act of 2005 because: (i) there are 100 or more class members, (ii) there is an aggregate amount in controversy exceeding $5,000,000, exclusive of interest and costs, and (iii) there is minimal diversity because at least one plaintiff and defendant are citizens of different states.

7. This Court also has supplemental jurisdiction over the state law claims pursuant to 28 U.S.C. § 1367.

8. Venue is proper in this judicial district and division pursuant to 28 U.S.C. § 1391. A substantial part of the events and/or omissions giving rise to the claims occurred within this district and division.

PARTIES

9. Plaintiff Patrick Ruffino is a resident of the state of Illinois.

10. On January 4, 2018, Plaintiff applied for, and subsequently received, a Capital One Secured Platinum Mastercard.

11. In order to apply for that card, Capital One required Plaintiff to provide his Personal Data, including but not limited to his address, social security number, date of birth, and his personal bank account number in order to "secure" the credit Capital One extended to him.

12. Plaintiff's Personal Data was compromised during the Breach Defendants made known on July 29, 2019.

13. Capital One has yet to directly inform Plaintiff (or any other Class members) of the Breach, or identify the categories of their Personal Data that were misappropriated due to Capital One's myriad IT failures.

14. The Breach already has required Plaintiff to expend significant time and energy to protect himself from the Breach's potential adverse consequences, including but not limited to investigating whether hackers misappropriated his Personal Data—since Capital One has yet to notify impacted customers—and potential means by which to protect himself from identity theft, and monitoring his linked bank account for fraudulent transactions.

15. Plaintiff has also requested that each of the three major credit reporting bureaus freeze his credit to guard against unauthorized efforts to establish credit accounts in his name.

16. Plaintiff would not have applied for a credit card with and provided Personal Data to Capital One had Capital One disclosed that it lacked adequate computer systems and data security practices to adequately safeguard his and other consumers' Personal Data.

17. As a direct and proximate result of the Breach, and Capital One's failure to prevent against and timely notify Plaintiff of the same, Plaintiff has suffered concrete injuries.

18. Plaintiff's damages also include the heightened risk of fraud and identity theft to which the Breach exposed him

19. Defendant Capital One Financial Corporation is an entity incorporated in the State of Delaware with its headquarters and principal place of business located at 1680 Capital One Drive, McLean, Virginia.

20. Defendant Capital One Bank (USA) is a subsidiary of Defendant Capital One Financial Corporation, and has its headquarters and principal place of business located at 1680 Capital One Drive, McLean, Virginia.

21. Defendant Capital One, National Association is a subsidiary of Defendant Capital One Financial Corporation, and has its headquarters and principal place of business located at 1680 Capital One Drive, McLean, Virginia.

22. Capital One Financial Corporates operates primarily through Defendants Capital One Bank (USA) and Capital One, National Association. Accordingly, all Defendants are jointly and severally liable for the harms complained of herein.

FACTUAL ALLEGATIONS

A. The Banking System is a Constant Target for Hackers

23. Data breaches have become a constant threat, routinely exposing consumer data to malicious actors.

24. In 2018, the Identity Theft Resource Center and CyberScout Annual End-of-Year Data Breach Report revealed a 126% increase in exposed consumer data, and 1.68 billion email-related credentials.[2]

25. Because of the valuable nature of the sensitive Personal Data consumers provide financial institutions, the banking sector is a particularly attractive target for cyber criminals; the banking sector reportedly experienced 135 data breaches in 2018 alone.[3]

26. As one public interest group has explained: "The risk of cyberattack on financial services firms cannot be overstated. Cyberattacks cost financial services firms more to address than firms in any other industry at $18 million per firm (vs. $12 million for firms across industries). Financial services firms also fall victim to cybersecurity attacks 300 times more frequently than businesses in other industries. In other words, while the typical American business is attacked 4 million times per year, the typical American financial services firm is attacked a staggering 1 billion times per year."[4]

---

[2]Identity Theft Resource Center, End of Year Data Breach Report (2018). Available at https://www.idtheftcenter.org/2018-end-of-year-data-breach-report/.

[3] *Id*.

[4] Forbes, *Laughing All The Way To The Bank: Cybercriminals Targeting U.S. Financial Institutions*, August 28, 2018. Available at https://www.forbes.com/sites/bhaktimirchandani/2018/08/28/laughing-all-the-way-to-the-bank-cybercriminals-targeting-us-financial-institutions/#f4bfefe6e906.

27. Identity thieves use stolen personal information to perpetuate a variety of crimes that harm consumers, including immigration fraud, obtaining a driver's license or identification card in the victim's name but with another's picture, using the victim's information to obtain government benefits, filing fraudulent insurance claims, fraudulently purchasing drugs or medical devices, filing a fraudulent tax return using the victim's information to obtain a fraudulent refund, fraudulently obtaining a loan tied to the victim's credit and personal information, and fraudulently opening credit accounts in the victim's name.

B. Capital One's Data Practices

28. Capital One requires all prospective customers who wish to obtain a credit card and other financial services to provide Personal Data in order to secure a credit account.

29. In addition, Capital One requires applicants seeking a "secure" Capital One credit account—typically consumers "with bad credit who are financially vulnerable"[5]—to provide sensitive bank account information in order to ensure Capital One is able to secure repayment of any credit extended thereto.

30. Capital One is obligated by law to retain the Personal Data Plaintiff and Class members submitted in connection with their applications.

31. Moreover, by obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class members' Personal Data, Capital One assumed legal and equitable duties to those individuals. Capital One knew or should have known that they were responsible for protecting Plaintiff's and Class members' Personal Data from disclosure. At all relevant times, Plaintiff and Class members had taken all reasonable steps to maintain the confidentiality of their Personal Data.

[5] https://www.nytimes.com/2019/07/30/business/capital-one-breach.html (last visited July 31, 2019.)

32. One of the nation's most prominent financial institutions, Capital One also undoubtedly knew the importance of safeguarding the Personal Data Plaintiff and others entrusted to it, and the tangible and intangible harms its customers likely would experience if its data security systems were breached.

33. Indeed, Capital One independently promised to safeguard Personal Data. Examples include:

> At Capital One, we make your safety and security a top priority and are committed to protecting your personal and financial information. If we collect identifying information from you, we will protect that information with controls based upon internationally recognized security standards, regulations, and industry-based best practices.[6]

> Safeguards are in place to protect your information.
> - We prohibit the unlawful disclosure of your Social Security number.
> - We restrict access to your Social Security number except when required for authorized business purposes.[7]

> We maintain physical safeguards, such as secure areas in buildings; electronic safeguards, such as passwords and encryption; and procedural safeguards, such as customer authentication procedures.[8]

34. Capital One failed to safeguard this information, however, and Plaintiff and Class' Personal Data has now fallen into the wrong hands.

C. The Breach

35. On or about July 29, 2019, Capital One announced that on "July 19, 2019, it determined that there was unauthorized access by an outside individual who obtained certain types of personal information relating to people who applied for its credit card products and to Capital One credit card customers."[9]

---

[6] https://www.capitalone.com/identity-protection/privacy/statement (last visited August 1, 2019)
[7] https://www.capitalone.com/applications/identity-protection/commitment/ (last visited August 1, 2019)
[8] *Id.*
[9] https://www.capitalone.com/facts2019/ (last visited July 31, 2019).

36. According to Capital One, the compromised Personal Data consists of sensitive personally identifiable information it routinely collects in connection with credit application processing, "including names, addresses, zip codes/postal codes, phone, email addresses, dates of birth, and self-reported income." [10]

37. Moreover, beyond the credit card application data, the Breach put at risk customer status data (e.g., credit scores, credit limits, balances, payment history, and contact information), fragments of transaction data from a total of 23 days during 2016-2018, about 140,000 Social Security numbers of credit card customers, and about 80,000 linked bank account numbers of secured credit card customers like Plaintiff.[11]

38. The announcement stated that the Breach affected consumers and small businesses who applied for a credit card product from 2005 through early 2019, approximately 100 million individuals in the United States.[12]

39. At no point in Capital One's statement did it offer Plaintiff and the Class concrete assistance to protect them from the dangers to which Capital One's systemic failures exposed them.[13]

40. Paige A. Thompson, the hacker, disseminated the Personal Data of approximately 100 million consumers by posting on her GitHub account on April 21, 2019 using the handle "erratic." This information was free and available to any user to download and use.[14]

[10] *Id.*
[11] *Id.*
[12] *Id.*
[13] *Id.*
[14] https://www.wired.com/story/capital-one-hack-credit-card-application-data/ (last visited July 31, 2019)

41. Capital One not only failed to prevent the Data Breach, but also failed to detect it. The Personal Data posted on Thompson's GitHub account remained exposed until at least July 17, 2019, when Capital One was informed by an unidentified tipster.[15]

42. In short, Capital One discovered the Breach by sheer happenstance; its purported physical, electronic and procedural safeguards failed not only to prevent the Breach, but also to detect it.

D. Capital One's Failure to Comply with Federal Requirements

43. The Federal Trade Commission ("FTC") has issued numerous guides for businesses highlighting the importance of reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-marking.[16]

44. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established guidelines for fundamental data security principles and practices for business.[17] The guidelines note businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand its network's vulnerabilities; and implement policies to correct security problems.[18] The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.[19]

---

[15] *Id.*
[16] Federal Trade Commission, *Start With Security*, available at https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf.
[17] Federal Trade Commission, *Protecting Personal Information: A Guide for Business*, available at https://www.ftc.gov/tips-advice/business-center/guidance/protecting-personal-information-guide-business.
[18] *Id.*
[19] *Id.*

45. Here, at all relevant times, Capital One was fully aware of its obligation to protect the Personal Data of its applicants, including Plaintiff and Class members' Personal Data, because it is one of the United States' largest financial institutions. Capital One was also aware of the significant consequences of its failure to do so because it collected applicant data from millions of consumers monthly (if not daily), and knew that this data, if hacked, would injure consumers, including Plaintiff and Class members.

46. Capital One's failure to follow the FTC guidelines, and its subsequent failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data constitutes an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 14 U.S.C. § 45.

E. Plaintiff and Class Members have Suffered Harm

47. Like any data hack, the instant Breach presents major problems for all affected. Said Jonathan Bowers, a fraud and data specialist at fraud prevention provider Trustev, "Give a fraudster your comprehensive personal information, they can steal your identity and take out lines of credit that destroy your finances for years to come."[20]

48. The FTC warns the public to pay particular attention to how they keep personally identifying information: Social Security numbers, financial information, and other sensitive data. As the FTC notes, "[t]hat's what thieves use most often to commit fraud or identity theft." And once they have this information, "they can drain your bank account, run up your credit cards, open new utility accounts, or get medical treatment on your health insurance."[21]

49. The ramifications of Capital One's failures to properly secure Plaintiff's and Class members' Personal Data are severe. Identity theft occurs when someone uses another person's

[20] http://www.cnet.com/news/data-breach-snags-data-from-15m-t-mobile-customers/ (last visited Oct. 6, 2015).
[21] https://www.consumer.ftc.gov/articles/0271-warning-signs-identity-theft (last visited July 31, 2019).

medical, financial, and personal information, such as that person's name, address, Social Security Number, medical and insurance information, financial account information, and other information, without permission to commit fraud or other crimes.

50. According to data security experts, one out of four data breach notification recipients became a victim of identity fraud.

51. Here, due to the Breach, Plaintiff and Class members have been exposed to injuries that include, but are not limited to:

a. Theft of personal and financial information;

b. Costs associated with the detection and prevention of identity theft and unauthorized use of financial accounts;

c. Damages arising from the inability to use debit or credit card accounts because accounts were suspended or otherwise rendered unusable as a result of fraudulent charges stemming from the Breach, including but not limited to foregoing cash back rewards;

d. Damages arising from the inability to withdraw or otherwise access funds because accounts were suspended, restricted, or otherwise rendered unusable as a result of the Breach, including, but not limited to, missed bill and loan payments, late-payment charges, and lowered credit scores and other adverse impacts on credit;

e. Costs associated with spending time to address and mitigate the actual and future consequences of the Breach, such as finding fraudulent charges, cancelling and reissuing payment cards, purchasing credit monitoring and identity theft protection services, imposition of withdrawal and purchase limits on compromised accounts, including but not limited to lost productivity and opportunities, time taken from the

enjoyment of one's life, and the inconvenience, nuisance, and annoyance of dealing with all issues resulting from the Breach;

f. The imminent and impending injury resulting from potential fraud and identity theft posed because their personal information is exposed for theft and sale on the dark web;

g. Damages to and diminution in value of the personal information entrusted to Capital One for the sole purpose of purchasing products and services from Capital One; and

h. The loss of Plaintiff's and Class members' privacy.

52. Moreover, the Personal Data compromised in the Breach has no expiration date. While credit card numbers and the like may become useless after some time, personal identification numbers and Social Security numbers do not. The United States government and privacy experts acknowledge that when such data is compromised, it may take years for identity theft to come to light.

53. Plaintiff and Class members has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from their Personal Data being placed in the hands of criminals.

54. As a direct and proximate result of Defendants' actions and omissions in disclosing and failing to protect Plaintiff's and Class members' private personal information, Plaintiff and those similarly situated have been placed at a substantial risk of harm in the form of identity theft, and have incurred and will incur actual damages in an attempt to prevent identity theft.

55. Plaintiff and Class members retain an interest in ensuring there are no future breaches in addition to seeking a remedy for the harms suffered as a result of the Breach for themselves and on behalf of similarly situated consumers who's Personal Data was stolen.

CLASS ALLEGATIONS

56. Plaintiff brings this action on behalf of himself and, pursuant to Fed. R. Civ. P. 23(a), 23(b)(2), and 23(b)(3), a class of

> All United States residents who applied for Capital One credit cards between 2005 and 2019 (the "Class").
>
> Excluded from the Class are Defendants, its executives, officers, and the Judge(s) assigned to this case.

Plaintiff reserves the right to modify, change or expand the Class definition after conducting discovery.

57. In the alternative, Plaintiff brings this action on behalf of himself and, pursuant to Fed. R. Civ. P. 23(a), 23(b)(2), and 23(b)(3), a subclass of

> All Illinois residents who applied for Capital One credit cards between 2005 and 2019 (the "Illinois Class").
>
> Excluded from the Illinois Class are Defendants, its executives, officers, and the Judge(s) assigned to this case.

58. Numerosity: The Class is so numerous that joinder of all members is impracticable. Defendants have acknowledged that the Breach compromised the Personal Data of approximately 100 million consumers.

59. Existence and Predominance of Common Questions of Fact and Law: Common questions of law and fact exist as to all members of the Class. These questions predominate over the questions affecting individual Class members. These common legal and factual questions include, but are not limited to:

a. whether Defendants' data security and retention policies were unreasonable;

b. whether Defendants failed to protect the confidential and highly sensitive information with which they were entrusted;

c. whether Defendants breached any legal duties in connection with the data breach;

d. Whether Defendants' conduct was intentional, reckless, willful or negligent;

e. whether Defendants were negligent;

f. whether Defendants were unjustly enriched;

g. whether Plaintiff and Defendants entered into a bailment arrangement, which was breached; and

h. whether Plaintiff and Class members are entitled to monetary damages, injunctive relief and/or other remedies and, if so, the nature of any such relief.

60. Typicality: All of Plaintiff's claims are typical of the claims of the Class since Plaintiff and all members of the Class had their Personal Data compromised in the Breach.

61. Adequacy: Plaintiff is an adequate representative because his interests do not materially or irreconcilably conflict with the interests of the Class that he seeks to represent, he has retained counsel competent and highly experienced in complex class action litigation, and he intends to prosecute this action vigorously. Plaintiff and his counsel will fairly and adequately protect the interests of the Class.

62. Superiority: A class action is superior to all other available means of fair and efficient adjudication of the claims of Plaintiff and members of the Class. The injury suffered by each individual Class member is relatively small in comparison to the burden and expense of

individual prosecution of the complex and extensive litigation necessitated by Defendants' conduct. It would be virtually impossible for members of the Class individually to effectively redress the wrongs done to them. Even if the members of the Class could afford such individual litigation, the court system could not. Individualized litigation presents a potential for inconsistent or contradictory judgments. Individualized litigation increases the delay and expense to all parties and to the court system presented by the complex legal and factual issues of the case. By contrast, the class action device presents far fewer management difficulties, and provides the benefits of single adjudication, economy of scale, and comprehensive supervision by a single court. Members of the Class can be readily identified and notified based on, *inter alia*, Defendants' records and databases. Indeed, Defendants claim to already be in the process of notifying them.

63. Defendants have acted, and refused to act, on grounds generally applicable to the Class, thereby making appropriate final relief with respect to the Class as a whole

CAUSES OF ACTION

COUNT I
BREACH OF IMPLIED CONTRACT
(On Behalf of the Nationwide Class or, Alternatively, the Illinois Class)

64. Plaintiff incorporates by reference each of the allegations contained in the foregoing paragraphs of this Complaint.

65. Capital One solicited and invited Plaintiff and Class members to apply for credit card products by providing their Personal Data. Plaintiff and Class members accepted Capital One's offers and provided their Personal Data to Capital One to apply for Capital One credit card products.

66. When Plaintiff and Class members applied for Capital One credit card products, they provided their Personal Data to Capital One. In doing so, Plaintiff and Class members entered into a mutually agreed-upon implied contract with Capital One wherein Plaintiff and Class members

agreed that their Personal Data was valid, while Capital One agreed that it would use Plaintiff and Class members' Personal Data in its possession for only the agreed-upon purpose of processing the credit card product application, and no other purpose.

67. Implicit in the agreement to use the Personal Data in its possession for only the agreed-upon application and no other purpose was the obligation that Capital One would use reasonable measures to safeguard and protect the Personal Data of Plaintiff and Class members in its possession.

68. By accepting the Personal Data for credit card product applications, Capital One assented to and confirmed its agreement to reasonably safeguard and protect Plaintiff's and Class members' Personal Data from unauthorized disclosure or uses and to timely and accurately notify Plaintiff and Class members if their data had been breached and/or compromised.

69. Plaintiff and Class members would not have provided and entrusted their Personal Data to Capital One to apply for the Capital One credit card products in the absence of the implied contract between them and Capital One.

70. Plaintiff and Class members fully performed their obligations under the implied contracts with Capital One.

71. Capital One breached the implied contracts they made with Plaintiff and Class members by failing to safeguard and protect Plaintiff's and Class members' Personal Data, and by failing to provide timely and accurate notice to them that their Personal Data was compromised as a result of the Breach.

72. Capital One breached the implied contracts it made with Plaintiff and Class members by failing to ensure that Plaintiff's and Class members' Personal Data in its possession was used only for the agreed-upon application verification and no other purpose.

73. Plaintiff and Class members conferred a monetary benefit on Capital One which has accepted or retained that benefit. Specifically, the credit card products typically carry annual fees and other charges (e.g. interest) for use. In exchange, Plaintiff and Class members should have received the services that were the subject of the transaction and should have been entitled to have Capital One protect their Personal Data with adequate data security measures.

74. Capital One failed to secure Plaintiff's and Class members' Personal Data and, therefore, did not provide full compensation for the benefit Plaintiff and Class members provided.

75. Capital One acquired the Personal Data through inequitable means when they failed to disclose the inadequate security practices previously alleged.

76. If Plaintiff and Class members had known that Capital One would employ inadequate security measures to safeguard Personal Data, they would not have applied for the Capital One credit card products.

77. As a direct and proximate result of Capital One's breaches of the implied contracts between Capital One and Plaintiff and Class members, Plaintiff and Class members have sustained actual losses and damages as described in detail above.

78. Plaintiff and Class members were harmed as a result of Capital One's breach of the implied contracts because their Personal Data was compromised, placing them at a greater risk of identity theft and subjecting them to identity theft, and their Personal Data was disclosed to third parties without their consent. Plaintiff and Class members also suffered diminution in value of their Personal Data because it is now easily available on the dark web.

79. Plaintiff and Class members have also suffered consequential out-of-pocket losses for procuring credit freeze and protection services, identity theft monitoring, late fees, bank fees, and other expenses relating to identity theft losses or protective measures. Plaintiff and Class

members are further damages as their Personal Data remains in the hands of those who obtained it without their consent.

80. This breach of implied contracts was a direct and legal cause of the injuries and damages to Plaintiff and Class members as described above.

COUNT II
NEGLIGENCE
(On Behalf of the Nationwide Class or, Alternatively, the Illinois Class)

81. Plaintiff incorporates by reference each of the allegations contained in the foregoing paragraphs of this Complaint.

82. Defendants had a duty to, *inter alia*, take reasonable measures to protect the Personal Data entrusted to them.

83. Defendants breached this duty by knowingly and intentionally failing to adequately safeguard the Personal Data of Plaintiff and Class members, or to take commercially reasonable measures to protect that Personal Data.

84. Defendants were legally obligated to timely disclose the Breach to Plaintiff and Class members.

85. Defendants failed to timely notify Plaintiff and Class members, thereby preventing Class members from taking meaningful, proactive steps to investigate possible identity theft.

86. In light of the recent data breaches in the news, it was reasonably foreseeable that its failure to safeguard this data would injure Plaintiff and Class members.

87. Defendants' breaches proximately caused harm to Plaintiff and Class members by placing them at a substantial risk of harm in the form of identity theft, and causing them to incur, or to incur in the future, actual damages in an attempt to prevent identity theft.

COUNT III
NEGLIGENCE, *Per Se*
(On Behalf of the Nationwide Class or, Alternatively, the Illinois Class)

88. Plaintiff incorporates by reference each of the allegations contained in the foregoing paragraphs of this Complaint

89. Section 5 of the FTC Act prohibits "unfair … practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Capital One, of failing to use reasonable measures to protect Personal Data. The FTC publications and orders described above also form part of the basis of Capital One's duty in this regard.

90. Capital One violated Section 5 of the FTC Act by failing to use reasonable measures to protect Personal Data, and not complying with applicable industry standards, as described in detail herein. Capital One's conduct was particularly unreasonable given the nature and amount of Personal Data it obtained and stored, and the foreseeable consequences of a data breach including, specifically, the immense damages that would result to Plaintiff and Class members.

91. Capital One's violation of Section 5 of the FTC Act constitutes negligence *per se*.

92. Plaintiff and Class members are within the class of persons that the FTC Act was intended to protect.

93. The harm that occurred as a result of the Data Breach is the type of harm the FTC Act was intended to guard against.

94. As a direct and proximate result of Capital One's negligence *per se*, Plaintiff and Class members have suffered, and continue to suffer, injuries, and damages arising from identity theft; damages from lost time and effort to mitigate the actual and potential impact of the Breach on their lives, including, *inter alia*, by placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, closely reviewing

and monitoring their credit reports and accounts for unauthorized activity, and filing police reports, and damages from identity theft, which may take months if not years to discover and detect, given the far-reaching, adverse and detrimental consequences of identity theft and loss of privacy.

95. Additionally, as a direct and proximate result of Capital One's negligence *per se*, Plaintiff and Class members have suffered and will suffer the continued risks of exposure of their Personal Data, which remain in Capital One's possession and is subject to further unauthorized disclosures so long as Capital One fails to undertake appropriate and adequate measures to protect the Personal Data in its continued possession.

COUNT IV
VIOLATION OF THE ILLINOIS CONSUMER FRAUD ACT
(815 CS 505/1, *et seq.*)
(On Behalf of the Illinois Class)

96. Plaintiff incorporates by reference each of the allegations contained in the foregoing paragraphs of this Complaint.

97. This count is brought against Defendants pursuant to the Illinois Consumer Fraud and Deceptive Trade Practices Act, 815, ILCS 505/1, et seq. ("ICFA").

98. At all times relevant herein, the ICFA was in effect. The ICFA prohibits "unfair and deceptive practices."

99. Plaintiff and members of the Class are consumers.

100. A violation of the Illinois Personal Information Protection Act ("IPIPA"), 815 ILCS 530/1, *et seq.*, "constitutes an unlawful practice under the [ICFA]." IPIPA § 20.

101. Defendants are "Data Collectors" within the meaning of IPIPA § 5.

102. The Breach experienced by Defendants constitutes a "breach of the security of the system data" within the meaning of IPIPA § 5.

103. Pursuant to the IPIPA, the sensitive and unencrypted customer information misappropriated from Defendants includes Plaintiff's and other Class members' "personal information," including names, Social Security numbers, and driver's license or state identification card numbers. IPIPA § 5.

104. Defendants have unreasonably delayed informing Plaintiff and members of the Class about the security breach of Class members' confidential and non-public information immediately following discovery of the same. The public notice provided generally to Plaintiff and the Class thus far also fails to comply with the specific notice requirements set forth in the Act. *See* IPIPA § 10(a)-(b). Defendants have therefore violated the IPIPA and engaged in unlawful practices in violation of the ICFA.

105. Defendants' violations of the ICFA proximately caused harm to Plaintiff and the Class by placing them at a substantial risk of harm in the form of identity theft, and causing them to incur, or to incur in the future, actual damages in an attempt to prevent identity theft.

106. Plaintiff and Class members also are entitled to recover their attorneys' fees, litigation expenses, and costs, under the ICFA.

COUNT V
BREACH OF CONTRACT
(On Behalf of the Nationwide Class or, Alternatively, the Illinois Class)

107. Plaintiff incorporates by reference each of the allegations contained in the foregoing paragraphs of this Complaint.

108. Plaintiff and Class members contracted with Capital One for the provision of credit cards, which required them to agree to Capital One's terms and conditions of service.

109. Capital One's terms and conditions incorporated by reference Capital One's privacy policy, in which it states that it will use "encryption and other technologies, such as

hashing, to de-identify data about a particular individual."

110. Capital One breached its agreements with Plaintiff and the Class by failing to use such measures to protect their Personal Data.

111. Defendant's breach of these obligations proximately caused harm to Plaintiff and the Class by placing them at a substantial risk of harm in the form of identity theft, and causing them to incur, or to incur in the future, actual damages in an attempt to prevent identity theft.

COUNT VI
UNJUST ENRICHMENT
(On Behalf of the Nationwide Class or, Alternatively, the Illinois Class)

112. Plaintiff incorporates by reference each of the allegations contained in the foregoing paragraphs of this Complaint. This count is plead in the alternative to the contract-based claims.

113. Plaintiff and the Class conferred a benefit upon Defendants, which was known and appreciated by them.

114. It would be inequitable for Defendants to retain this benefit under the circumstances of this case.

COUNT VII
BAILMENT
(On Behalf of the Nationwide Class or, Alternatively, the Illinois Class)

115. Plaintiff incorporates by reference each of the allegations contained in the foregoing paragraphs of this Complaint. This count is plead in the alternative to the contract-based claims.

116. Plaintiff and Class members delivered and entrusted their Personal Data to Defendants for the sole purpose of receiving services from them.

117. During the time of bailment, Defendants owed Plaintiff and Class members a duty to safeguard this information properly, and to maintain reasonable security procedures and practices to protect such information. Defendants breached this duty.

118. Defendants' breaches proximately caused harm to Plaintiff and the Class by placing them at a substantial risk of harm in the form of identity theft, and causing them to incur, or to incur in the future, actual damages in an attempt to prevent identity theft.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of himself and members of the Class, respectfully requests that this Court:

A. Determine that the claims alleged herein may be maintained as a class action under Rule 23 of the Federal Rules of Civil Procedure, and issue an order certifying the Class as defined above;

B. Appoint Plaintiff as the representative of the Class and her counsel as Class counsel;

C. Award all actual, general, special, incidental, statutory, and consequential damages to which Plaintiff and Class members are entitled;

D. Award pre-judgment and post-judgment interest on such monetary relief;

E. Grant appropriate injunctive and/or declaratory relief;

F. Award reasonable attorneys' fees and costs; and

G. Grant such further relief that this Court deems appropriate.

DEMAND FOR JURY TRIAL

Plaintiff respectfully demands a trial by jury on all issues so triable.

Dated: August 2, 2019

Respectfully submitted,

By: *s/ Daniel O. Herrera*

Daniel O. Herrera
Christopher P.T. Tourek
CAFFERTY CLOBES MERIWETHER & SPRENGEL LLP
150 S. Wacker, Suite 3000
Chicago, Illinois 60606
Telephone: (312) 782-4880
Facsimile: (312) 782-4485
Email: dherrera@caffertyclobes.com
ctourek@caffertyclobes.com